



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/677,933	10/01/2003	Richard H. Boivie	YOR920030398US1 (8728-647)	9603
46069 7590 12/23/2010 F. CHAU & ASSOCIATES, LLC Frank Chau 130 WOODBURY ROAD WOODBURY, NY 11797				
EXAMINER ALMEIDA, DEVINE E				
ART UNIT 2432		PAPER NUMBER		
NOTIFICATION DATE 12/23/2010		DELIVERY MODE ELECTRONIC		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mail@chauiplaw.com
garramone@chauiplaw.com
uspto1@chauiplaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte RICHARD H. BOIVIE and WILLIAM ERIC HALL

Appeal 2009-006972
Application 10/677,933
Technology Center 2400

Before LANCE LEONARD BARRY, HOWARD B. BLANKENSHIP,
and THU A. DANG, *Administrative Patent Judges*.

DANG, *Administrative Patent Judge*.

DECISION ON APPEAL¹

¹ The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the “MAIL DATE” (paper delivery mode) or the “NOTIFICATION DATE” (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

I. STATEMENT OF CASE

Appellants appeal the Examiner's final rejection of claims 11, 13, 14, 16-19, and 22-28 under 35 U.S.C. § 134 (2002). Claims 1-10, 12, 15, 20, and 21 have been canceled. We have jurisdiction under 35 U.S.C. § 6(b) (2008).

A. INVENTION

According to Appellants, the invention relates to a secure computing device that protects its secrets and its integrity using hardware mechanism and advanced cryptographic techniques (Spec. 1, ll. 5-7).

B. ILLUSTRATIVE CLAIM

Claim 11 is exemplary and is reproduced below:

11. A method for ensuring that a processor will execute only authorized code, said method comprising:

reading a certificate including a first public key into a protected memory;

validating said certificate with a second public key permanently stored on said processor;

reading a signed authorized code into said protected memory, wherein said protected memory is cryptographically protected;

preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key; and

branching to a copy of said signed authorized code in said protected memory to begin execution and performing

inline decryption of the copy of said signed authorized code in said protected memory upon verifying said digital signature.

C. REJECTIONS

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Sudia	US 2001/0050990 A1	Dec. 13, 2001
Morgan	US 6,185,685 B1	Feb. 06, 2001

Claims 11, 13, 14, 16, 18, and 22-26 stand rejected under 35 U.S.C. § 102(b) over the teachings of Sudia.

Claims 17, 19, 27, and 28 stand rejected under 35 U.S.C. § 103(a) over the teachings of Sudia and Morgan.

We affirm.

II. ISSUE

The issue is whether Appellants have shown that the Examiner erred in finding that Sudia discloses “verifying a digital signature used to sign said signed authorized code in accordance with said first public key” as required by claim 11.

III. FINDINGS OF FACT

The following Findings of Fact (FF) are shown by a preponderance of the evidence.

Sudia

1. Sudia discloses a third party upgrade, wherein the manufacturer signs a firmware upgrade certificate containing a public key of the third

- party firmware provider and issues it to that third party (pg. 22, ¶ [0249]).
2. The third party develops, tests, and approves replacement or additional firmware routines, signs the routines with the third party's private signature key, and attach its upgrade certificate from the manufacturer thereto (*id.*).
 3. Upon receiving the upgrade, the user loads both the signed code routines and the manufacturer's upgrade certificate into the device, wherein the device would then verify the third party's signature on the new code routines against the manufacturer's upgrade certificate (*id.*).

IV. ANALYSIS

35 U.S.C. § 102(b)

In the Appeal Brief, Appellants contend that “Sudia does not teach ‘preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key’ as claimed in Claims 11 and 22” (App. Br. 6). In particular, Appellants argue that “the manufacturer’s signature of Sudia is not analogous to the claimed first public key” (*id.*).

However, the Examiner finds the following in Sudia:

In an instance of third party upgrade, the manufacturer could sign a firmware upgrade certificate containing a public key (i.e. certificate including a first public key) of the third party firmware (i.e. first public key) provider and issue it to that third party. The third party could then develop, test, and approve replacement or additional firmware routines, sign them with the third party's private signature key (i.e. signed authorized code), and attach its upgrade certificate (i.e. certificate including a first public key) from the manufacturer thereto.... The device would then *verify the third party's signature on the new code*

routines (i.e. signed authorized code) against the manufacturer's upgrade certificate (i.e. certificate including a first public key).

(Ans. 8-9, citing Sudia).

In response to the Examiner's Answer, Appellants additionally contend in the Reply Brief that "[t]he device of Sudia does not perform the desired upgrade until the manufacturer's public signature is used to verify the manufacturer's upgrade certificate" and that "Sudia's upgrade is not performed upon *verifying the third party's signature* essentially as claimed" (Reply Br. 9). Furthermore, Appellants contend that "[t]he new code routines are not *executed* as claimed" and thus "the executed user issued instructions of Sudia are not implemented with the certificate" (*id.*).

However, such additional arguments in the Reply Brief are not commensurate in scope with the language of representative claim 11. That is, contrary to Appellants' arguments (Reply Br. 9), claim 11 does not recite any such "upgrade... performed upon *verifying the third party's signature* essentially as claimed" (emphasis added). In fact, claim 11 does not require that the new code routines are "executed" as Appellants contend (*id.*). That is, claim 11 merely requires "preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key" (emphasis added).

We give the claim its broadest reasonable interpretation. *See In re Bigio*, 381 F.3d 1320, 1324 (Fed. Cir. 2004). Moreover, we will not read limitations from the Specification into the claims. *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993).

Claim 11 does not place any limitation on what "preparing to execute said signed authorized code" means, includes, or presents other than it is

done “by verifying a digital signature used to sign said signed authorized code.” Accordingly, we interpret such preparing step to comprise “verifying a digital signature used to sign said signed authorized code” as specifically defined in claim 11. That is, we will not read performing upgrade “upon verifying the third party’s signature” or implementing “the executed user issued instructions” with the certificate into claim 11, as Appellants contend (Reply Br. 9, emphasis added).

In Sudia, the manufacturer signs a firmware upgrade certificate containing a public key of the third party firmware provider (FF 1). Accordingly, we find Sudia to disclose a certificate including a first public key.

In Sudia, the third party signs the updated firmware routines with the third party’s private signature key and attach its upgrade certificate from the manufacturer thereto (FF 2), wherein the receiving device would then verify the third party’s signature on the new code routines against the manufacturer’s upgrade certificate (FF 3). We find Sudia’s new code routines to comprise code, wherein Sudia’s third party’s signature for the routines read on a digital signature used to sign authorized code of claim 11. Similarly, we find the third party’s public key enclosed in the manufacturer’s upgrade certificate reads on the first public key.

Thus, we find Sudia also discloses verifying a digital signature used to sign authorized code with the first public key, as specifically required by claim 11. That is, in view of our claim construction above, we find no error with the Examiner’s finding that Sudia discloses “preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key” (claim 11). Accordingly, we find that Appellants have not

shown that the Examiner erred in rejecting representative claim 11, claims 22 and 23 falling therewith, and claims 13, 14, 16, 18, and 24-26 depending from claims 11 and 23 respectively, under 35 U.S.C. § 102(b) over Sudia.

35 U.S.C. § 103(a)

As for claims 17 and 19 depending from claim 11 and claims 27 and 28 depending from claim 23, Appellants merely argue that “[t]he dependent claims are believed to be allowable for at least the reasons given for the respectively independent claims” (App. Br. 8). As discussed above, we find no deficiencies in Sudia and thus find that the Examiner did not err in rejecting independent claims 11 and 23. Accordingly, we hold that the Examiner did not err in rejecting claims 17, 19, 27 and 28 depending respectively therefrom under 35 U.S.C. § 103(a) over Sudia in view of Morgan.

V. CONCLUSION AND DECISION

The Examiner’s rejection of claims 11, 13, 14, 16, 18 and 22-26 under 35 U.S.C. § 102(b) and claims 17, 19, 27 and 28 under 35 U.S.C. § 103(a) is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

peb

F. CHAU & ASSOCIATES, LLC
FRANK CHAU
130 WOODBURY ROAD
WOODBURY, NY 11797